

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 04-199246
(43)Date of publication of application : 20.07.1992

(51)Int.Cl. G06F 12/14

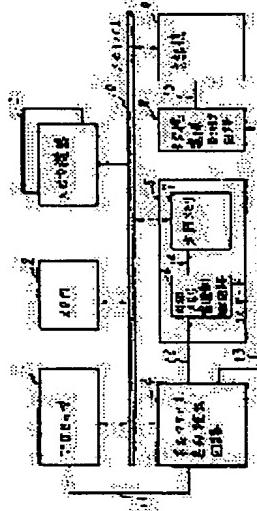
(21)Application number : 02-317800 (71)Applicant : HITACHI LTD
(22)Date of filing : 26.11.1990 (72)Inventor : TORII SHUNICHI

(54) HIGHLY RELIABLE STORAGE SYSTEM

(57)Abstract:

PURPOSE: To easily erase the content of a semiconductor storage device in a short time irrespective of the capacity of the storage device by generating a power supply stopping signal upon detecting illegal access and stopping the power supply to the storage device in response to the power supply stopping signal.

CONSTITUTION: An illegal access and life detecting device 4 detects the occurrence of an illegal access request by monitoring memory reference requests on a memory bus 10 and also detects the expiration of designated life time by means of a timer mechanism. Upon detecting such abnormality, the device 4 instructs the internal memory power supply control circuit 6 and main storage power supply control circuit 8 of an IC card 5 to stop power supply through control lines 12 and 13. When the power supply is stopped, the contents of the main storage 9 of a DRAM and internal memory 7 of the SRAM of the IC card 5 are instantaneously erased. Therefore, the contents is easily erased at a high speed irrespective of the capacity of the storage devices.



⑫ 公開特許公報 (A)

平4-199246

⑬ Int.CI.⁵

G 06 F 12/14

識別記号

320 A

厅内整理番号

8841-5B

⑭ 公開 平成4年(1992)7月20日

審査請求 未請求 請求項の数 3 (全5頁)

⑮ 発明の名称 高信頼化記憶システム

⑯ 特 願 平2-317800

⑰ 出 願 平2(1990)11月26日

⑱ 発明者 鳥居 俊一 東京都国分寺市東恋ヶ窪1丁目280番地 株式会社日立製作所中央研究所内

⑲ 出願人 株式会社日立製作所 東京都千代田区神田駿河台4丁目6番地

⑳ 代理人 弁理士 小川 勝男 外1名

明細書

1. 発明の名称

高信頼化記憶システム

2. 特許請求の範囲

1. 半導体記憶装置と記憶装置電源制御回路と不正な記憶装置アクセスを検出する装置によりなり、上記不正な記憶装置アクセスを検出する装置は、不正なアクセスの検出に応じて電源停止信号を生成し、上記記憶装置電源制御回路は、上記電源停止信号に応じて、上記半導体記憶装置への電源の供給を停止することを特徴とする高信頼化記憶システム。

2. 半導体記憶装置と記憶装置電源制御回路と記憶寿命検出装置によりなり、

上記記憶寿命検出装置は寿命の尽きたことを検出した時、電源停止信号を生成し、上記記憶装置電源制御回路は、上記電源停止信号に応じて、上記半導体記憶装置への電源の供給を停止することを特徴とする高信頼化記憶システム。

3. バックアップ電池により内部メモリに電源を

供給するICカードにおいて、

内部メモリへの電源供給を強制的に停止する機構を有することを特徴とするICカード。

3. 発明の詳細な説明

【産業上の利用分野】

本発明は記憶装置の内容の保全に好適な機構に関するものである。

【従来の技術】

半導体記憶装置は高速で簡便なアクセスが可能であるが、逆に内容を第三者が簡単に読出したり、変更したりすることが可能である。例えばICカードは、個人の情報を記憶する極めて小型の記憶装置でバックアップ電源の機構により長時間内容を保持出来るものであるが、盗難等により簡単に第三者の手に渡る恐れがある。内容の不正な読出しには、パスワード等の機構もあるが多回の試行で破られてしまう場合が多く完全とはいえない。又、主記憶装置の例では、一時的に作成した情報も積極的に内容を消去しなければ第三者から情報を盗まれる可能性もある。

〔発明が解決しようとする課題〕

従来技術ではこのような状態において、記憶装置上に情報が保持されていること自体が逆に問題であり、なんらかの手段で、内容を簡単に消去してしまえば内容の漏洩は完全に防ぐことが出来る。

〔課題を解決するための手段〕

記憶装置に不正なアクセスやあらかじめ決められた時間以上経過したことを検出する回路を設け、その指示により記憶装置の電源供給を断つことにより上記消去は簡単に実現される。

〔作用〕

書き換えが可能なDRAMやSRAMのような半導体記憶素子は電源の供給が短時間でも断たれればその内容を失う揮発性の性質がある。従来はこの性質は欠点と看されることが多く、バックアップ電源機構の付加により克服されている。しかし、本発明ではこの性質を利用して、記憶装置の容量によらない高速かつ簡便な消去方法を実現している。

〔実施例〕

またタイマ機構により経過時間が指定寿命時間以上になったことも検出出来る。このような異常を検出したときには不正アクセス・寿命検出装置4は、制御線12及び13を介して、ICカードの内部メモリ電源制御回路6及び、主記憶電源制御回路8に電源の供給停止を指示する。DRAMの主記憶9及びICカードのSRAMの内部メモリ7は、電源の停止により瞬時にその内容を失う。

第2回は、不正アクセス・寿命検出装置4の詳細な構成の1例を示したものである。領域属性定義テーブル30は、主記憶やICカードの内部メモリの各領域の属性の定義情報を格納したテーブルである。属性としては、(1)命令語参照の禁止／許可、(2)オペランド参照の禁止／許可、

(3)書き込みの禁止／許可の3つが各領域に定義される。メモリバス10上には、アドレス10-1のほかに、命令語参照／オペランド参照の区別10-2、書き込み要求か否かの区別10-3も送出されている。領域属性定義テーブル30にアドレス10-1を入力すると、参照領域の属性

以下、本発明の実施例を第1図以降をもじいて説明する。

第1図は本発明の1実施例の記憶サブシステムを組み込んだ計算機システムの全体構成である。メモリバス10を介して、プロセッサ1、OS等を格納した読み専用メモリ(ROM)2、各種入出力機器3及び記憶システムとして、DRAMで構成された主記憶9、ICカード5(第1図では、ICカードとメモリバスの接続は直接つながる構成例を示してあるが、ICカード接続装置を介しても良い)及び本発明の主要部である不正アクセス・寿命検出装置4が接続されている。主記憶電源制御回路8は主記憶9に電力線15を介して電源を供給する回路である。ICカード5内のSRAMで構成された内部メモリ7の電源は、バックアップ電池を内蔵した内部メモリ電源制御回路6より供給されている。

不正アクセス・寿命検出装置4は、メモリバス10上のメモリ参照要求をモニタリングすることにより不正なアクセス要求の発生を検出出来る。

が信号線43、44、45上に得られる。ANDゲート群及び反転ゲート31により、ANDゲート32からは命令語領域への不正なオペランド参照検出信号、ANDゲート33からはオペランド領域への不正な命令語参照検出信号、ANDゲート34からは書き込み禁止領域への不正な書き込み要求検出信号が得られる。信号線11-1は、第1図に示したプロセッサ1から不正アクセス・寿命検出装置4への制御線の1部であり、ROM2上のICカード参照権限チェックプログラム(第4図に詳細を説明する)の指示により、ICカードのパスワードチェックに失敗したことを通知する信号線である。

信号線43、44、45及び11-1はいずれも記憶装置への不正な参照を検出したことを通知する信号線である。これを契機にただちに、記憶装置の内容を消去するとプログラムのバグ等の過失によっても簡単に消去されてしまい不都合である。本実施例ではこのような状況の発生をORゲート35で集めた後、カウンタ36で回数を記憶

する。不正要求の回数を、レジスタ37にあらかじめ設定された許容回数と比較回路38により比較し、許容回数を超えたとき、ORゲート41と信号線12、13を経由して電源停止要求が送出される。

第3図は、ICカードの内部メモリ電源制御回路6の詳細な実施例を示したものである。ICカードが計算機に接続されていないときには、電源切換装置50を経由してバックアップ電池よりわずかなSTAND-BY電流が内部メモリに供給され、内容が保持される。なお、線53は電源のグランドとなる接地線である。ICカードが計算機に接続されたときには、計算機システムからの電源が外部電源として計算機本体より電力線52を経由して供給される。この時は、内部メモリには電力線52からの電流が、電源切換装置50を経由して内部メモリに供給される。ゲート54は内部メモリへの電流を制御するもので、信号線12から停止要求がある間は、電流を切断する。主記憶電源制御回路8も第3図と同一の回路で実

現出来る。バックアップ電池が不要であれば、ゲート54だけの更に簡単な回路で実現できることは明らかである。

第2図のタイマ回路40は、情報の寿命を検出するためのものであり、一定時間が経過すると満期の信号を信号線42の送出し、ORゲート41を経由して停止信号を送出する。

第2図の領域属性定義テーブル30、レジスタ37、タイマ回路40はプロセッサより樹には示していないが制御線群11を経由して初期値設定や更新が可能である。

第4図はICカード参照権限チェックプログラムの詳細を示したものである。このプログラムはICカード中の暗号化されたパスワード情報とユーザの入力したパスワードの一一致を調べるものである。一致すれば許可を回答する。不一致であれば三回までユーザの再入力を許しそれでも失敗したときには禁止を回答する。本発明との関係で重要な点は、不一致が判明したときステップ64で、不正アクセス・寿命検出装置4にパスワードチエ

ックに失敗したことを通知している点である。

本実施例では、不正アクセスの検出に専用回路（領域属性定義テーブル30、ANDゲート32、33、34）を使用しているが、プロセッサ本体の記憶保護回路の出力を利用出来れば、それでも勿論良い。同様に、寿命検出のタイマ40の替わりにプロセッサ内部のタイマ機能を利用しても良い。更に、不正アクセス・寿命検出装置4全体の機能を実現するプログラムをROM2上に付加する実現方式も可能である。

本実施例ではICカードには内部メモリ7と内部メモリ電源制御回路6のみを内蔵した構成を示したが、他の部分例えば、不正アクセス・寿命検出装置4もICカードに内蔵されても良いし、第1図に示した全ての回路がICカード内蔵されていても勿論良い。

【発明の効果】

第1図以降に示した実施例によれば、盗まれたICカードの内容を読み出そうとしても、パスワード入力を何度か試みるうちにカウンタ36が回

数を記憶する。不正要求の回数が許容回数を越えれば、内容が瞬時に自動的に消去出来る。パスワード入力失敗回数をICカード自体に記録し多数回の試行を禁止する方式に比べても、機密情報を消去できる点で本発明はより安全である。

別の効果としては、ウイルスの拡散防止にも利用できる。入出力機器3よりウイルスを含んだプログラムが主記憶又はICカードの内部メモリにロードされても、ウイルスは拡散するために、自プログラム以外の命令語領域や本来はオペランド領域であるはずの領域に、ウイルスの種を書き込みそこで実行したりするので、不正アクセス・寿命検出装置4により不正参照が検出できる。検出されれば、ウイルスを含んだプログラムやウイルスの種も同時に消去され、ウイルスの拡散が防止できる。

更に別の効果としては、ICカードに一定時間だけ有効なプログラムを置くことが出来る。プログラム中の命令語だけを格納してある領域をオペランド参照禁止に定義すれば、コピーしようと

してもオペランド参照となり不正参照が検出出来き、続行すれば I C カードの内容そのものが消去される。従ってコピーすることが出来ない。寿命検出機能により指定時間を経過すれば自動的に消去される。この機能により一定期間のレンタルプログラムが実現できる。利用者は、レンタル店で自分の I C カードに試用してみたいプログラムを書き込んでもらい、自宅で第1図に示す計算機システムでそれを実行する。寿命機能によりプログラムは一定時間後に自動的に消去されるので、返却のために利用者はレンタル店に訪れる必要が無い。書き込みについても課金の仕組があれば、ネットワークを利用してレンタル店に訪れる必要も無くなる。この効果を利用する場合には、I C カードごとに寿命を設定したいので、不正アクセス・寿命検出装置 4 を I C カードに内蔵する構成が適当である。寿命の検出としてはタイマの他にも、メモリ読みだしの回数、I C カードを接続している時間だけを計測するタイマ等の変形も考えられる。

又更に別の効果としては、共通に利用する計算機システムに適用すれば、不用意に主記憶上に残した個人の機密情報を一定時間後には必ず消去されるので、他人に盗まれる危険性が減少する。勿論 O S は、ユーザが主記憶上に残した個人の機密情報を、別のユーザにそのまま渡さない仕組を有している。しかしその消去は、別のユーザに主記憶を割り当てる直前まで実行を送らせていている場合が多く、積極的に消去する本発明を利用すればより安全となる。

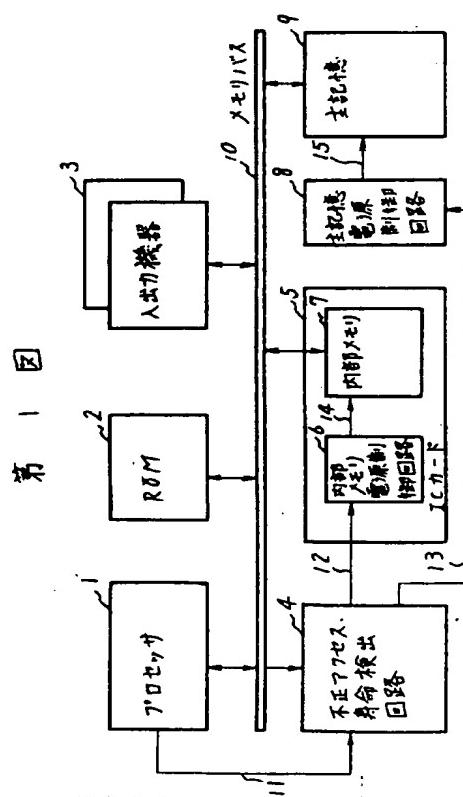
記憶装置の消去をプロセッサからの命令により順次ゼロクリアする方式に比べ、本方式は特別なプログラムが不要なだけでなく記憶装置の容量によらず短時間に内容を消去出来る利点がある。

4. 図面の簡単な説明

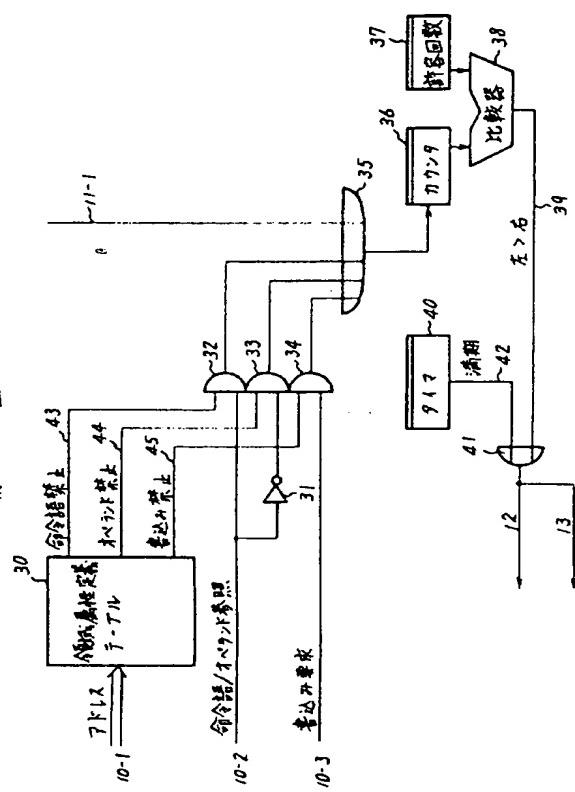
第1図は本発明の記憶システムが適用された計算機システムの全体構成図、第2図は不正アクセス・寿命検出装置 4 の構成図、第3図は I C カードの内部メモリ電源制御回路 6 の構成図、第4図は I C カード参照権限チェックプログラムのフロ

一図である。

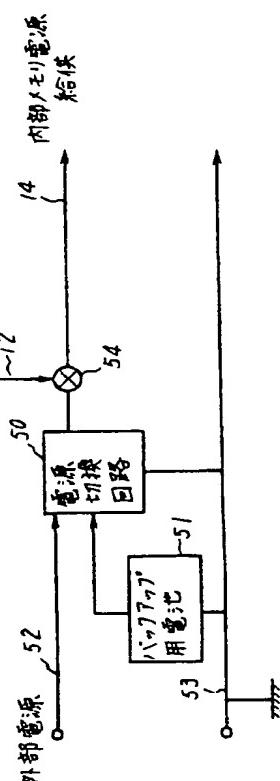
代理人 弁理士 小川勝男



22



3



第 4

